Appendix Q

ITO Historical Workload

This report documents the following ITO historical workload trends:

- 2013 Incident and Request Workload – by Priority
- 2014 Incident and Request Workload – by Priority
- Enterprise Ticket Metrics – DMDC
- Top Fifteen Request Areas – 2014

2013 Incident and Request Workload – by Priority

Ticket Type	Priority	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sept	Oct	Nov	Dec	Grand Total
Incident Tickets	1-Emergency	1	1	0	0	0	1	0	0	0	4	0	1	**8**
	2-Critical	4	6	1	2	5	3	4	9	1	4	6	1	**46**
	3-Urgent	396	303	475	534	781	721	360	391	285	725	390	408	**54**
	4-Routine	726	640	776	903	1043	977	1020	1068	819	890	966	831	**10659**
Incident Total		**1127**	**950**	**1252**	**1439**	**1829**	**1702**	**1384**	**1468**	**1105**	**1623**	**1362**	**1241**	**16482**
Ticket Type	Priority	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sept	Oct	Nov	Dec	Grand Total
Request Tickets	1-Emergency	1	0	0	1	3	1	2	5	3	1	1	4	**22**
	2-Critical	9	5	22	4	2	11	2	11	14	18	7	4	**109**
	3-Urgent	91	84	91	116	80	101	69	82	123	67	86	87	**1077**
	4-Routine	1655	1664	1462	1379	1481	1077	1259	1192	1029	1371	1148	965	**15682**
Request Total		**1756**	**1753**	**1575**	**1500**	**1566**	**1190**	**1332**	**1290**	**1169**	**1457**	**1242**	**1060**	**16890**
Grand Total		**2883**	**2703**	**2827**	**2939**	**3395**	**2892**	**2716**	**2758**	**2274**	**28467**	**2604**	**2301**	**58759**

Appendix Q

2014 Incident and Request Workload – by Priority

Ticket Type	Priority	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sept	Oct	Nov	Dec	**Grand Total**
Incident Tickets	1-Emergency	1	0	0	0	1	0	0	1	1	2	0	3	**9**
	2-Critical	0	9	7	3	2	6	3	6	14	17	7	3	**77**
	3-Urgent	389	654	360	628	472	358	408	931	1752	937	669	699	**8257**
	4-Routine	915	991	882	859	905	877	961	1152	1375	1067	446	674	**11104**
Incident Total		**1305**	**1654**	**1249**	**1490**	**1380**	**1241**	**1372**	**2090**	**3142**	**2023**	**1122**	**1379**	**19447**
Ticket Type	Priority	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sept	Oct	Nov	Dec	**Grand Total**
Request Tickets	1-Emergency	2	1	2	1	3	3	3	2	3	4	2	1	**27**
	2-Critical	10	5	14	6	19	13	17	8	50	26	9	16	**193**
	3-Urgent	62	80	86	95	60	63	81	85	126	161	51	101	**220**
	4-Routine	992	1081	1298	1423	1331	1394	1536	1339	1649	1767	679	1225	**15714**
Request Total		**1066**	**1167**	**1400**	**1525**	**1413**	**1473**	**1637**	**1434**	**1828**	**1958**	**741**	**1343**	**16985**
Grand Total		**2371**	**2821**	**2649**	**3015**	**2793**	**2714**	**3009**	**3524**	**4970**	**3981**	**1863**	**2722**	**33139**

Enterprise Ticket Metrics - DMDC

12 Month Workload Volumes & Distribution (01/2014 – 01/2015)

- Total Ticket Volume for 2014: 44,722
  - *Overall growth rate average:* 16% *Increase* from 2013-2014
    - Incident/Problem: 20,364 *(includes auto-event tickets)*
    - Service Requests: 17,676
    - Change Orders: 6,682 *(includes EAF tickets)*
  - *Projected growth for CY-2015: 18%*

Appendix Q

- Tier-1 Tickets (Help Desk/Service Desk): 12% of total *(FCR for this volume is approx. 85-90%)*

- Tier-2 Tickets (Desktop / User Support): 28% of total
- Tier-3 Tickets: 60% of total
    - Level-3 Teams Include: Production Support, Software Configuration Management, Oracle (Web/DB), Network/Telecom, Unix, Virtualization. Does *not* reflect Project resource workload.
    - Tier 3 level tickets require a higher degree of complexity, resources requirements and longer lifecycle time.

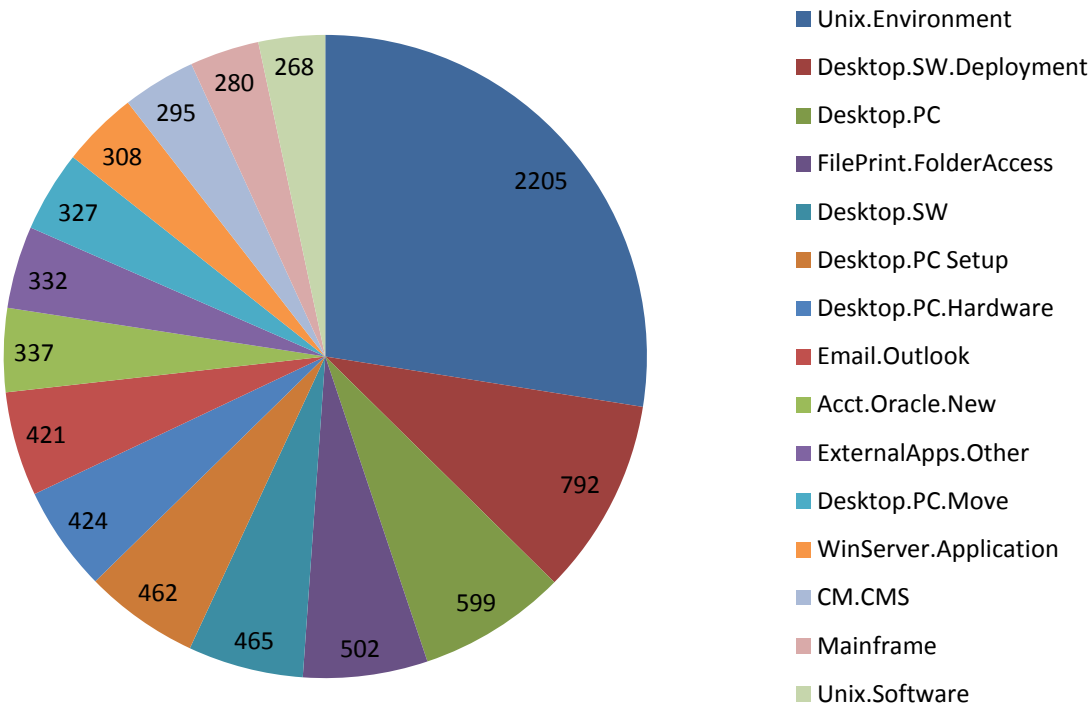
Appendix Q

Top Fifteen Request Areas - 2014

Summary:

This report contains the top fifteen Request and Incident areas reported in CA Service Desk during 2014. Each category was queried, documented, and noted with a brief analysis.

The Top 15 Year to Date Request Areas



Appendix Q

Analysis:

The top fifteen request areas made up 26% of the total reported tickets within CA Service Desk. Individual percentages for each request area are documented below. Percentages within the posted chart indicate percentages within the top fifteen request areas only.

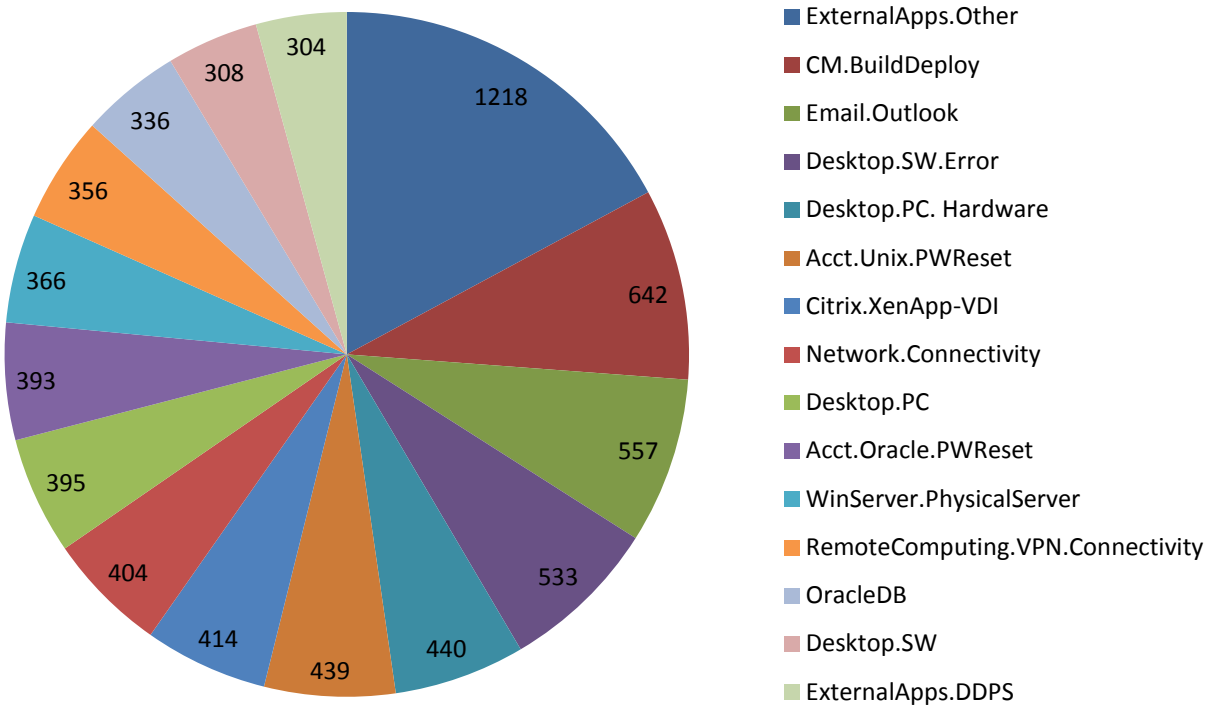
Request Area	Analysis
Unix.Environment – 7.2%	The majority of these requests were for space additions; server restarts due to unreachable servers, accessibility/login issues, or software installs needed for backup; and requests to apply OS patches. Patch related prep-work requests also made up a fair amount of the Unix.Environment requests.
Desktop.SW.Deployment – 2.6%	The majority of these requests were for users that did not have necessary software available in their software catalogs and reinstalling software that was lost following PC re-images.
Desktop.PC – 2%	There were various PC related issues logged under this request. These requests consisted of and were not limited to PC and PC peripheral device replacements, PC re-images, picking up and securing Systems FedEx packages, PC inventory and part recovery, access to virtual machines, installing second hard drives.
FilePrint.FolderAccess – 1.6%	The majority of these requests were for server, directory, and folder access. Organization email mailboxes also require approved File Access Action Forms and made up some of these requests.
Desktop.SW – 1.5%	The majority of these requests were individual user software deployment requests and were accompanied with the proper approved Software Request Form when approval was required. This request area also served as a catch all for several issues ranging from vulnerability scans to PC re-imaging requests and software updates.
Desktop.PC.Setup – 1.5%	The majority of these requests were for PC upgrades, PC images and deployments for desk sharing/hot-desking at the Mark Center, PC images for Ft. Knox, and visitor offices setups.
Email.Outlook – 1.4%	The majority of these requests were distribution list modifications (adding/removing list members), recovering certificates following CAC card replacements, adding mailboxes to user profiles, setting up new user profiles, and creating new organization mailboxes and distribution lists as a result of the DMDC Re-organization.
Desktop.PC.Hardware – 1.4%	This request area was a catch all for various PC hardware requests.

Appendix Q

	Requests consisted of second hard drives (most of these users are developers), PC re-imaging, additional memory, keyboard and monitor replacements, and second monitors. Several requests were also logged to track DRMO preparations and the replacement of defective APC power strips.
Acct.Oracle.New – 1%	The majority of these requests stemmed from the DSC migration from Beauregard to Ft. Knox. DSC Ft. Knox personnel require Oracle AUSR accounts in order to perform their job functions.
Desktop.PC.Move – 1%	The majority of these requests were due to the Mark Center desk sharing/hot-desking project, Lorton PC migration onto the DMDC network, asset moves for DRMO, and tracking the movement of equipment from the loading dock and other storage areas.
ExternalApps.Other – 1%	The majority of these tickets were requests for manual web application deployments, bouncing/restarting web applications due to errors or accessibility issues, and log level modifications. These requests were made across all environments.
WinServer.Application – 1%	The majority of these requests were WinServer patches, software install requests on various servers, assists with remediating vulnerabilities on WinServers, capturing shares and share permissions, and removal of backup agents.
CM.CMS – 0.9%	The majority of these requests were CMS access requests, CMS release modification forms, and prototype requests.
Mainframe – 0.9%	The majority of these tickets are RACF permissions requests. The majority of the permissions requests were for read only or update/alert permissions within various groups and files.
Unix.Software - 0.8%	The majority of these requests were for updating Linux and Solaris servers with current recommended OS patches and TeamQuest startups and upgrade/installations. Several requests were also submitted requesting SCC scans and executing SCC tool on JPAS servers.

Appendix Q

The Top 15 Year to Date Incident Areas



Appendix Q

Analysis:

The top fifteen incident areas made up 23% of the total reported tickets within CA Service Desk. Individual percentages for each request area are documented below. Percentages within the posted chart indicate percentages within the top fifteen incident areas only.

Incident Area	Analysis
ExternalApps.Other – 3.8%	This incident area served as a catch all for various errors, outages, and application issues reported within the Model Office, Test, Demo, and Production environments. The majority of these issues are assigned to and resolved by the Production Support team.
CM.BuildDeploy – 2.1%	The majority of these incidents were CM notifications of web application build and deployment failures. These issues were reported to and resolved by the DMDC CM Team.
Email.Outlook – 1.8%	The majority of these incidents were issues with sending and opening encrypted email, profile configuration issues, and DISA related outages. In 2014, there was a huge decrease in overall latency and "Not responding" issues in comparison to 2013.
Desktop.SW.Error – 1.7%	This incident area served as a catch-all for a broad range of issues, and there is not a specific incident that stands out as a majority. Issues range from but are not limited to users unable to sign or open PDF documents, Corestreet Validation errors, and application login errors.
Desktop.PC.Hardware – 1.4%	The majority of these incidents reported PCs that would not boot, PC latency, hibernation/sleep mode issues, issues with peripheral devices (CAC reader, mouse, keyboard, monitor), and toner replacements.
Acct.Unix.PWReset – 1.4%	All tickets submitted under this incident area were for Unix account password resets within various Unix servers. Resets were due to password expirations, forgotten passwords, and failed password attempts. Resetting the passwords restored user access.
Citrix.XenApp-VDI – 1.4%	The majority of these incidents were for hung sessions and users that were unable to access or launch the VDI portal. There was an influx of VDI users stemming from the DSC migration from Beauregard to Ft. Knox. Ft. Knox was not on the DMDC domain, and remote access was required in order for DSO, DSC, and PSA users at Ft. Knox to access the DMDC network. There were repeat reports of Ft. Knox users' inability to access VDI (connecting via terminal servers was a successful workaround). The root cause was found to be a policy change or update at the Ft. Knox site

Appendix Q

	for McAfee. Ports were opened, and the number of VDI access issues decreased significantly.
Network.Connectivity – 1.3%	The majority of these incidents were caused by tripped port security, VLAN moves, a west coast proxy device issue, and route table issue at Beauregard.
Desktop.PC – 1.3%	This incident area served as a catch-all for a broad range of issues, and there is not a specific incident that stands out as a majority. Issues range from but are not limited to Corestreet Validation errors, application login errors, PC login errors, scanner and printer issues, and hibernation/sleep mode issues.
Acct.Oracle.PWReset – 1.3%	All tickets submitted under this incident were for Oracle account password resets within various Oracle databases. Resets were due to password expirations, forgotten passwords, and failed password attempts. Resetting the passwords restored user access.
WinServer.PhysicalServer – 1.2%	The majority of these incidents were unreachable servers that required restarts, hung user session terminations, reports of low space on network drives in which additional space was released to resolve, and repeat issues with Hobbes.
RemoteComputing.VPN.Connectivity – 1.2%	The majority of these incidents were due to VPN outages and reports of latency. A Remote Computing Questionnaire was established to capture user feedback. The Questionnaire is available on SharePoint.
OracleDB – 1.1%	The majority of these incidents were to report databases that were down, database access issues, and Oracle account password resets.
Desktop.SW – 1%	This incident area served as a catch-all for a broad range of issues, and there is not a specific incident that stands out as a majority. Issues range from but are not limited to users unable to sign or open PDF documents, run time errors, application login errors, and missing network drives
ExternalApps.Other – 0.9%	This incident area served as a catch all for various errors, outages, and application issues reported within the Model Office, Test, Demo, and Production environments. The majority of these issues are assigned to and resolved by the Production Support team.